HSPD-12 Frequently Asked Questions
August 15, 2006

GENERAL

What is HSPD 12?
HSPD 12 is a presidential directive requiring all Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.

Does HSPD-12 apply to all agencies including the smaller agencies (e.g. micro-agencies)?
For the most part, yes. The Directive applies to all "Executive departments" and agencies listed in title 5 U.S.C. § 101, and the Department of Homeland Security; "independent establishments" as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201). The exceptions are as follows: "Government corporations" as defined by title 5 U.S.C. § 103(1) are encouraged, but not required to implement this Directive. (Ref: OMB M-05-024 Section 1.A.)

What is FIPS 201?
FIPS 201 is the Standard identified in HSPD-12 that sets out the requirements for a Federal government-wide identity credential for employees and contractors.

Why is the standard divided into 2 parts?
The standard is divided into two parts so agencies can make an orderly migration—in terms of both technology and "identity proofing" from their current systems to the requirements established by the standard and meet the deadlines established by the President in HSPD 12. Part 1 deals with the security objectives as they apply to uniform personnel identity proofing and vetting activities, while Part 2 focuses on the technical interoperability requirements, including the issuance of compliant identity badges and the implementation of the government-wide infrastructure to support the effective use of the badges. After October 27, 2006, reference to Part 1 and Part 2 of the Standard is obsolete.

What are the primary requirements for an agency to implement FIPS 201?
Revise the identity proofing and identity card issuance process of the agency to meet FIPS-201 requirements and implement access control mechanisms for facilities and IT systems that utilize the capabilities of the compliant identity credential. FIPS 201 requirements include the issuance of an identity badge that utilizes smart card technology, both contact and contactless, and incorporates a standardized Card Holder Unique Identifier (CHUID), digital credentials, and biometric templates.

Can federal agencies use the standard for other purposes beyond the scope of the standard to include national security applications?
Yes. The Directive specifically tasks agencies to identify additional applications important to security for which the standard might be employed. Such wider use must conform to Office of Management and Budget (OMB) policy (including the relevant privacy provisions) and, if national security systems are involved, the applicable requirements to protect national security information and systems.

What will the card look like?
Card topology is described and pictured in the Standard. Each card will contain a required set of information: a printed picture of the cardholder, name, expiration date, and agency affiliation. Additional optional information (e.g., signature, agency seal, issue date, etc.) may be selected by each agency within the parameters set by the Standard and further refined by OMB, where applicable.

Which agencies are responsible for government-wide activities associated with implementing the directive?
Four federal agencies have specific responsibilities for implementing this directive: Department of Commerce (DOC) for development of the Standard, OMB for oversight of agency implementation and development of policy, General Services Administration (GSA) for acquisition assistance, FBI for National Criminal History (Fingerprint) checks, and Office of Personnel Management (OPM) for assisting agencies with required background investigations.

What should agencies do to reduce the costs of HSPD-12 implementation?
To reduce costs, agencies must be prepared to share implementation processes as much as is feasible for each specific agency’s situation. OMB established an HSPD 12 Executive Steering Committee to provide strategic direction for implementing HSPD-12 using a government-wide strategy. Federal agencies are encouraged to consider the Shared Services solution as a means of reducing costs.

What should small agencies be doing right now?
Both large and small agencies will benefit from the government-wide strategy. Interested agencies should make their interest in a shared solution known to the GSA Managed Service Office (MSO). Once a decision has been made to participate, agencies will need to sign an MOU with GSA and prepare to transfer funds. FY2006 funds must be transferred to GSA by September 29, 2006.

What does "logical access" mean in FIPS 201?
Logical access, as used in FIPS 201, refers to use of the credential as part of identification and authentication processes that are used by automated information systems access authorization processes (e.g., log on actions and digital signatures).

How can agencies assess their existing infrastructure to tell if they are FIPS 201 compliant? Do you have any specific publication (like 800-53)?

FIPS 201 is the governing Standard for HSPD-12 compliance. FIPS 201 contains normative references to additional documents. Enrollment and Card Issuance processes may be assessed in accordance with SP 800-79. Data objects produced by Card Issuance system can be tested according to SP 800-85B, assisted by the 800-85B test toolkit. Implementation of infrastructure for utilizing the cards is covered by FISMA reporting and SP 800-53. (Ref: http://csrc.nist.gov/publications/nistpubs/index.html).

POLICY

Are waivers to the standard allowed?
There is no provision for waivers to standards issued by the Secretary of Commerce under the Federal Information Security Management Act of 2002. HSPD 12 also does not provide a waiver provision.

Is it OMB's and NIST's intent that agencies conduct investigations on and issue PIV/smart cards to large numbers of construction contractors (e.g., brick layers, plumbers, welders, etc.) who are responsible for construction of buildings on federal property, where the construction time exceeds 6 months?
OMB Memorandum 05-24 indicates that contractors will need badges if they will be routinely accessing government facilities and/or IT Systems on a regular basis for a period in excess of 6 months. It is up to the employing agency whether any particular contractor employee fulfills these criteria and must therefore be put through the FIPS-201 badging process. (Ref: OMB M-05-24 Sections 1.C, 7.F)

How is agency compliance monitored and what happens if an agency does not comply?
Like many other agency activities, oversight is the responsibility of each agency, the Office of Management and Budget, the Government Accountability Office, and oversight committees of Congress. NIST is responsible for providing a conformance test program to help agencies comply with FIPS 201. Information on the conformance program is available at http://csrc.nist.gov/piv-program. Non-compliance may include a range of consequences from negative audit reports to budgetary impacts. More importantly, agencies that do not comply will not meet the President’s goals of secure and reliable identification for federal employees and contractors.

What are the funding sources for agency implementation of FIPS 201?
All federal agencies have existing background investigation, access control, and identification credential activities. It is anticipated that these activities, and the funding used to support them will be used in support of activities compliant with FIPS 201. Any additional funding needs for implementing FIPS 201 should be requested by agencies through the normal federal budget process.

How many times can an applicant reapply before a permanent denial is issued?
Denial of credential issuance is based on the adjudication of a background investigation. Once an unfavorable result has been received, the issuance of a PIV credential is denied.

Individuals who receive unfavorable suitability determinations may appeal the decision to the Merit System Protection Board. (Ref: Title 5 CFR Part 731 Subpart E)

If there are employees and contractors working for another Federal agency working on contracts or services that support the tenant agency, can a PIV be issued by the agency whose property they work on or does the PIV have to be issued by the employing agency. Example: GSA provided maintenance support working in the building but the GSA office is not on site.
The authorization for card issuance should originate with the employing agency (or contracting agency in the case of contractors). However, there is nothing to prohibit one agency from providing issuance services to another agency in accordance with interagency MOA/MOU.

Does HSPD-12 require that a PIV credential be issued before a new employee is granted any access to Federal facilities or information systems?
No. Agencies may, at their discretion, issue new employees temporary ID badges for access while PIV enrollment and card issuance is in process. These temporary badges must be physically and electronically distinguishable from PIV credentials.

Can a PIV card be used by other organizations for other purposes (e.g., access to private facilities, identification for airline travel)?
HSPD-12 and FIPS-201 do not impose any restrictions on the use of the PIV card as an identity credential.

Is a Special Agreement Check (SAC) necessary or recommended in order to fulfill the FIPS 201 investigative mandate?
No. The investigative requirements set forth in FIPS 201 can be fully met through the use of existing suitability and national security investigations conducted by OPM and other agencies.

Can agencies use other investigative service providers in lieu of OPM to conduct the investigations required by FIPS 201?
No, unless an agency has original or OPM delegated authority to conduct background investigations. Contractor investigations must follow FIPS 201 and agency employee investigation processes.

Must reinvestigations be conducted to keep PIV credentials valid?
No. PIV credentials do not require reinvestigations to remain valid. Agencies must, however, continue to comply with the reinvestigative requirements set forth in the national security investigative standards.

If a person holds a PIV credential at one agency, and transfers to another agency, is a new investigation required?
No. Adjudicated investigations are acceptable across agency boundaries. The exception would be for increases in the risk or sensitivity levels of the new position, but these would be driven by existing suitability and/or national security investigative standards, not by FIPS 201 requirements specifically.

If a person has had a "break in service" (i.e., left a job for which they had to be investigated to meet FIPS 201 requirements), must a new investigation be conducted for that person to receive a new PIV credential?
If the "break in service" is two years or more, a new investigation must be conducted before a PIV credential can be issued. If the break in service is less than two years, an updated security questionnaire should be completed and any admitted issues resolved as appropriate.

Do all standard HSPD-12 requirements and guidance apply to a PIV credential issued to a foreign national living overseas?
Yes. All PIV credentials must be issued based on the same criteria. A working group was convened to develop specific controls for PIV issuance to foreign nationals living overseas. The policy for addressing PIV issuance for foreign nationals will be issued by October 2006.

For the PKI Credentials, are Registration Practices Agreements, additional Certificate Policies, or other methods of qualifying certificates use supported/encouraged/discouraged?
FIPS 201 and the Common Policy do not prohibit inclusion of additional certificate policies, (non-critical) private extensions, or extended key usage OIDs in the certificates. An agency can add whatever local information they need to the certificate; the agency cannot count on relying parties outside of the agency to recognize or honor that information. The Federal Common Policy Framework has been provided as a standard trust anchor for FIPS-201 implementation. When reliance on a certificate is required or optionally chosen, Federal Relying Parties are expected to employ due diligence in tracing the certificate 'path' to ensure the credential can be trusted, e.g. it uses the Common Policy Framework as its trust anchor. It is an Information Technology Security responsibility to ensure the relying party application is properly configured to accept or reject credentials based on these trust relationships. (Ref: OMB M-05-24, Section 4.D)

For questions on HSPD 12 policy, you may contact Carol Bales, OMB Senior Policy Analyst, on 202-395-9915.

HSPD-12 EXECUTIVE STEERING COMMITTEE

What is the Executive Steering Committee?
The HSPD-12 Executive Steering Committee (ESC) was established by OMB to provide strategic direction to the government-wide implementation of HSPD-12 and FIPS-201. The ESC is chaired by OMB and consists of executive sponsors from GSA, USDA, DOD, DHS, VA, DOC, DOI and USDA.

How will the HSPD-12 Executive Steering Committee address legacy identity management and building access systems and interfaces with agency access systems?
An architectural working group is developing a set of standard interfaces between the shared systems and the agency specific components (such as the building access systems). However, a large number of internal processes will remain the purview of the implementing agency.

What are the objectives of the HSPD-12 ESC?
As established by the HSPD-12 ESC Charter, the objectives of the HSPD-12 ESC are to:

- reduce the total Federal cost of HSPD-12 implementation;
- establish shared government-wide service infrastructure, policies, and procedures;
- establish a mechanism for small agencies to procure HSPD-12 services (either from an agency or through outsourcing);
- recommend solutions for sharing resources to ensure agencies meet the October 2006 HSPD-12 deadlines; and
- ensure government-wide interoperability.

Will the recommendations developed by the ESC meet agency specific requirements?
To achieve government-wide interoperability and cost savings, some compromises will be necessary between the agreed upon government-wide requirements and agency specific needs. Some agency specific needs will be accommodated, some will not. The ESC working groups will develop these requirements, based on agency feedback.

HSPD-12 SHARED SERVICES SOLUTION

What is the HSPD-12 Shared Services Solution?
The HSPD-12 Shared Services Solution is a contract vehicle sponsored by GSA for providing turn-key and other services in support of HSPD-12 implementation.

What specific shared services will be available, and when? Will they offer enrollment/ registration stations? What about PIV Card production?
The Shared Services solution includes end-to-end credential issuance beginning with presentation of an applicant’s identity documents through the issuance of a fully compliant PIV badge, and follow-on life-cycle maintenance of that credential. Specific services that are included in the Shared Services are enrollment, identity management, card management, card production (printing & personalization), PKI, and issuance. Background Investigations (NACI or equivalent), System Integration, Physical Access Control Systems, and Logical Access Control Systems are not included and remain the responsibility of the participating agency/

What locations will these shared services cover?
The Government Shared Services solution is taking a nationwide approach to providing card issuance and lifecycle maintenance services. On October 27, 2006, the program will

start with four cities. These have been identified as Seattle, Washington; Atlanta, Georgia; New York City, New York; and Washington, DC. The intent is to deploy up to 450 enrollment stations across the US within local proximity of 80% of the Federal workforce. Specific locations for enrollment station deployment will be provided to participating agencies during the rollout planning phase. The extent of the shared services rollout will be based on agency interest in shared services.

How much will shared services cost?
Specific costs will be available in August 2006. There are two types of expenses: Infrastructure and Card issuance/maintenance. The infrastructure will be a one time expense calculated on the number of participating agencies and their size. The card issuance/maintenance costs will be calculated on a per seat basis and will be an annual recurring expense.

Which agencies are offering to be shared service providers?
Government Shared Services will be provided by the General Services Administration and the Department of the Interior. The Department of State currently supports eight small agencies and is expected to continue to do so; however, they will not be a shared service provider as defined here. This is true also for the civilian uniformed services supported by the Department of Defense. (Ref: http://idmanagement.gov/drilldown.cfm?action=hspd12_mso)

Has a HSPD 12 compliant system been deployed to a production environment? If not, when is the compliant system scheduled to be deployed?
A compliant HSPD 12 system has not yet been deployed. In September 2006, GSA plans to demonstrate the HSPD-12 compliant systems as part of the shared services program, and deploy a fully compliant system in the production environment by October 27, 2006.

If agencies are sharing resources (e.g. card printing and registration), how will funding be shared and/or transferred between agencies?
GSA is establishing a Managed Service Offering for providing support to the Shared Services approach. There are two types of expense: the one-time infrastructure cost and the recurring per seat costs. Agencies participating in the Shared Services will be asked to contribute to the infrastructure as a price of admission, per seat costs will be assessed on an annual recurring basis.

What services will the GSA Managed Service Offering provide?
The MSO will manage the transfer of funds and acquisition of products and services in accordance with MOUs; however, oversee delivery and implementation; provide COTR and CO responsibilities for HSPD 12 products and services; and provide reporting back to agencies on status, etc.

What documents do agencies have to sign in order to obligate FY 2006 funds? Is this an interagency agreement?
Yes, this is an interagency agreement between GSA and the participating agency. An MOU will be provided by GSA for signature. Participating agencies will be asked to

provide some financial information for the funds transfer. For a copy of the MOU, go to the GSA Managed Service Office link:
http://idmanagement.gov/drilldown.cfm?action=hspd12_mso.

How will participation in the Shared Solution Impact the agency's HSPD-12 Implementation Plan?
OMB will be issuing a request for updated implementation plans from the agencies to be due in September 2006. In August 2006, those agencies participating in the Shared Solution should indicate this in their revised plans and to what extent they will be participating.

Under the Shared Services Solution, will the system owner(s) provide to affected agencies the Privacy Impact Assessments (PIA) and System Certification and Accreditation (C&A) (SP 800-37) and Process C&A (SP 800-79) Accreditations Memorandums?
The system owner(s), once identified, will conduct a PIA and both required accreditations. The PIAs will be posted on GSA's website and the full C&A assessment reports will be available to agencies for review upon request.

Will agencies be able to acquire services using agency contract vehicles? Or, will OMB direct agencies to use only the GSA solution?
OMB requires agencies to acquire only approved PIV products and services. Such products and services may be acquired through GSA IT Schedule 70, SIN 132-62. If acquired through other acquisition vehicles, agencies must maintain an ongoing plan and ensure products and services acquired conform to all applicable federal standards and requirements for the lifecycle of the components.

Can Agencies participate in the shared services program for some aspects of the shared services offering, but "go it alone" for others? Can an agency enter into an agreement to utilize shared services for certain geographical locations but not for others?
Yes. Agencies may pick and choose from the shared service offerings. They may also choose to participate based on specific geographic locations. However, agencies should be aware there may be some accretion in costs for these partial, or ‘unbundled,’ services.

For agencies participating in the Shared Services solution, will the personal identifying information of agency personnel be stored in a single government-wide database? If so, what steps are being taken to mitigate privacy and security concerns?
No. The Shared Services Identity Management System (IDMS) will keep individual agency information in separate and distinct databases. The information captured in this IDMS will be limited to the set of data required for card issuance and management. Complete personnel records will separate and distinct from this IDMS and will continue to reside in the Human Resources Line of Business, or in the employing agency. A Privacy Impact Assessment of the shared services IDMS will be conducted to ensure all necessary safeguards is employed.

Do internal agency hiring practices have to be changed or standardized in order to use the shared services?
FIPS-201 places certain new requirements on the background investigations conducted as part of an agency's hiring and contracting processes. The Shared Services solution does not impose any additional requirements beyond these other than the requirement for a 'sponsor' to initiate the card enrollment by providing information to the IDMS, and the requirement for the adjudication official to notify the IDMS when the background investigation is complete and successfully adjudicated.

For questions on the GSA MSO, you may contact the MSO, on 703-872-8646, or e-mail the MSO at HSPD12@gsa.gov.

IMPLEMENTATION

What documents/programs are currently available to help agencies implement FIPS 201?

- NIST Special Publication 800-73 specifies PIV card interface characteristics.
- NIST Special Publication 800-76 specifies PIV card biometric characteristics.
- NIST Special Publication 800-78 specifies cryptographic algorithm requirements and characteristics
- NIST Special Publication 800-79 provides guidance for PIV issuer accreditation.
- OMB M-05-24 provides implementation guidance on HSPD-12
- GSA memorandum of August 10, 2005 specifies the procedures for ordering goods and services in compliance with the Presidential Directive.
- NIST Special Publication 800-85 provides conformance tests for validating PIV components as complying with SP 800-73.
- NIST Special Publication 800-87 contains codes for the identification of Federal and federally-assisted organizations, needed in PIV identifiers.
- OMB M-05-24 provides policy guidance and deadlines supplementary to HSPD-12.
- OMB M-06-18 provides updated acquisition guidance to Federal agencies.
- Federal Identity Management Handbook
- Smart Card Handbook

Is there a list of "approved" identity proofing and registration processes?
There is not a list of "approved" identity proofing and registration processes, per se. "Approved" means that the process has met the control objectives, and the head of the agency has approved in writing that the process does meet the objectives. SP 800-79 provides further guidance on the certification and accreditation of PIV card issuing organizations. (See FIPS-201, Section 2)

Is Personal Identity Verification different from access authorization such that having a PIV card or achieving identity verification does not automatically entitle the cardholder to physical or logical access?

Yes. Access control remains the purview of the local facility or IT system security policy.

Will agencies maintain records of access to facilities by individuals?
This is outside the scope of the standard. It can be anticipated that agencies will continue to maintain records, in accordance with the Privacy Act, of access to and unsuccessful attempts to access their facilities and systems as required for their security and audit needs.

Does compliance to FIPS 201 mean that every door in every federal building and every federal computer terminal must have a PIV card reader?
No. Generally, agencies will implement FIPS-201 access controls on facility access points (i.e. entry doors) first. Further deployment within the facility is at the discretion of the agency facility security manager. Logical access controls are recommended for IT Systems operating at E-Authentication Level 3 or higher. As agencies develop their plans in accordance with HSPD 12, they should focus on the highest-risk facilities and systems for initial deployment of readers. Over time, this could expand to lower-risk systems and facilities. (Ref: OMB M-04-04, DOJ Vulnerability Assessment of Federal Facilities Report - June 1995, ISC Security Design Criteria for New Construction and Major Modernizations - December 2004 and Security Standards in Leased Space - Jan 2005.)

Is a 2.5mm border where printing is not permitted required for the topology of the card?
Yes. Compliance with the dimensions specified in FIPS 201 is required.

Does the PIV Sponsor, Registrar, PIV Card Approval and the PIV issuer have to be all different people or can one person have multiple roles?
FIPS-201 requires that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person. Therefore, separation of roles is required. At the very least, the Sponsor and the Authorizing Official must be separate and distinct individuals. The process for achieving separation of roles is the responsibility of the implementing agency. (Ref: FIPS 201 Section 2.2)

What format is required for the enrollment record (which encapsulates biometric records, document scans, demographic information, etc.)?
The standards permit individual departments and agencies to select the format most appropriate to their operations.

Does Registrar record signing only apply to pen-and-paper records, or does it also apply to electronic enrollment records?
The requirement applies to both paper and electronic storage. The method is left to individual departments and agencies. If cryptographic signature processes are employed, they must conform to the requirements of NIST standards and guidelines.

During reissuance, if an attribute has changed, who is responsible for verifying the change and recording the change and the reason for it?
This function is best performed by the Registrar since this is the individual rechecking the

records during card re-issuance. However, this is open to individual agency discretion which may choose to utilize an alternative process.

Is support for PIV card logical access mandatory on enrollment systems and/or issuance systems? If so, is PIV card verification required for all operator logins?
Credential-based identification support is specified in FIPS 201. Use of the identity credentials for specific access control applications is not. However use of a PIV card to verify Registrar, Sponsor, Approval, or Issuer roles for card issuance activities as an on-going activity would be an effective mechanism for maintaining the security of the process.

Do PIV enrollment systems need to communicate directly with PIV Digital Signatories, PIV issuance systems or any other satellite systems, or is it expected that all of this will be conducted via the IDMS?
This will vary based on individual agency implementations.

Will PIV enrollment systems be expected to send Electronic Fingerprint Transmission Specification (EFTS) records directly to the FBI Integrated Automated Fingerprint Identification System (IAFIS), or is that a function that will be handled by the IDMS?
This will vary based on individual agency implementations.

For the facial image, is there a specific color backdrop that should be used?
There is no backdrop color requirement; however, per the recommendation of the International Committee for Information Technology Standards (INCITS) 385, the background should be uniform.

Can identity proofing be conducted by federal employees and also "trusted agents," where trusted agents might include contractors?
FIPS 201 does not prohibit contractors from being employed to conduct identity proofing activities under the supervision of government employees in accordance with departmental or agency security and contracts management policies.

How can agencies receive an advance report of the fingerprint check results?
Agencies who receive their investigations from OPM, may obtain advance reports of fingerprint check results by putting the code "R" in the Codes block of the Agency Use section of any of the standard investigative forms (SF-86, SF-85P, or SF-85).

How will implementation of HSPD-12 and FIPS 201 affect OPM's current case service timeliness? Is OPM prepared for this workload?
Almost all investigations which will be required by HSPD-12, and which otherwise would not have been required, will be on uncleared contractors. Currently, many of these persons are being investigated already by agencies with the resources to do so. Further, no one is certain as to the exact number of these persons. Therefore, the aggregate amount of new investigations attributable to HSPD-12 cannot be known, but it will be something less than the number of uncleared government contractors. OPM is ready to

accept the additional investigations this policy will create. Since the NACI (National Agency Checks and Inquiries investigation), the minimum investigation required by FIPS 201, is not a field-investigative case type, no significant impact on the timeliness of service is anticipated.

What standard is to be used for adjudicating investigations conducted to meet the basic FIPS 201 requirements?
5 CFR 731 provides the basic suitability adjudication criteria. OPM can provide additional guidance regarding the adjudication process. National security investigations are adjudicated in accordance with guidance promulgated by Executive Order 12968.

As of October 2006, what capabilities is an agency required to have in place? Do agencies have to use the card's capabilities (e.g. at the highest security location in the agency?) Is the use of the card optional?
On October 27, 2006, agencies must begin issuing FIPS 201 compliant identity badges. OMB's HSPD 12 implementation guidance does not require agencies to complete implementation of all card capabilities on October 27, 2006. Agencies are not expected to have their entire infrastructure installed to enable use of the card at all facilities and systems. Agencies are expected to make use of the cards using a risk-based approach and phase in use of the card capabilities. Agencies will see a greater return on investment by using the cards to secure their facilities and systems.

Does the FIPS 201 standard include a physical access control system?
No. FIPS 201 does not specify the physical access control system (PACS). In order to effectively implement HSPD-12, each agency will need to implement a PACS for internal use. The Smart Card Interagency Advisory Board has published Technical Implementation Guidance Smart Card Enabled Physical Access Control System (TIG SCEPACS) 2.2 as a guide to assist agencies in this implementation, which is referenced by FIPS 201.

How much will it cost agencies to implement FIPS 201?
The cost will vary by agency depending upon how well its current identification credential program already meets the requirements of the new standard and the level of difficulty or complexity to migrate to the new standard. Some costs (e.g., understanding requirements, initiating projects) are fixed; some (e.g., PIV card readers, PIV card issuer facilities) are proportional to the number of facilities and systems involved; some (e.g., PIV cards, PIV card issuance) are proportional to the number of employees involved. The HSPD-12 ESC-sponsored Managed Service Offering will assist agencies in cutting costs by pooling resources and sharing infrastructure.

GSA ACQUISITION SERVICES AND PRODUCT EVALUATION PROGRAM

Do the individual vendors need to conclude negotiations with GSA to place their products onto the schedule?

Vendors with approved products will need a contract with GSA on IT Schedule 70 in order to provide product listing on SIN 132-62, or be listed by a reseller who has the item listed on SIN 132-62.

Why does GSA have the responsibility to perform FIPS201 product evaluation?
The Evaluation Program directly supports the acquisition process for implementing HSPD-12. OMB Memorandum M-05-24 designates GSA as the “executive agent for Government-wide acquisitions of information technology” under section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. § 11302(e)). (Ref: OMB M-05-24, Section 5.B.)

Why are some products/services not represented by a category on the FIPS201 Product/Service category list?
There are several products/services that may be necessary for HSPD-12 systems and deployments, but have no normative requirements specified in FIPS 201 and, therefore, are not included in the FIPS 201 Evaluation Program (e.g., integration services, contractor managed services and solutions). Qualification requirements for these services and a list of qualified vendor services are also posted at: http://idmanagement.gov.

What is the relationship between GSA and NIST as it pertains to the Product/Service Evaluation Program?
NIST is the authority for the Standard from which GSA derived the product/service categories and the evaluation criteria for each. The NIST FIPS 201 and FIPS 140 Conformance Testing and Certification is a component of the evaluation process for those categories of products designated to require conformance testing. NIST Conformance Testing and the GSA evaluation process can be conducted simultaneously; however, the product will not be placed on the approved product list until both have been successfully completed. The categories that require NIST certification include the template matcher, template generator, biometric functionality, the card itself, PIV middleware, and the cryptographic functionality.

The download ZIP file from the GSA FIPS 201 Evaluation Product for these products includes a non-disclosure agreement (NDA) with Atlan Laboratories of McLean, VA. Is Atlan the “Lab” that is referenced in the approval procedure documents associated with these products?
Yes, Atlan Laboratories is currently GSA’s FIPS 201 Evaluation Laboratory.

On the FIPS 201 Evaluation Program website, vendors are only allowed one user per "logon". The site explains that this is due to "sensitive" and "intellectual" property. Can GSA elaborate on what is meant by "sensitive" and "intellectual property"?
Sensitive or intellectual property is anything that the vendor feels affects their competitive edge. Examples of this type of data could be the vendor’s evaluation criteria, or GSA’s evaluation of the vendor’s product. A single control point for this type of data prevents inadvertent disclosure to unauthorized individuals. In addition, GSA finds it streamlines information flow.

Since some companies may have several lines of business administered by different sectors of their organizations, can one user "logon" be applied on a "per line of business" basis?
There is flexibility in the program for such situations. GSA permits vendors to provide justification for multiple log-on points of contact, where applicable.

If a product is certified in one brand of product, but not another (e.g., a finger print sensor algorithm) will it have to be reevaluated and recertified for the second product?
No, provided the documentation indicates that this is the same product, e.g. manufacturer and part number are identified and consistent.

Will the participants in the MINEX test receive some sort of letter in which they can pass on to GSA?
After the successful completion of tests on template generators and template matchers, NIST will post notices to the MINEX Compliant List at the Ongoing MINEX web site http://fingerprint.nist.gov/minex/. GSA will consult the MINEX Compliant List as part of the evaluation process.

If a supplier is listed by NIST as having a MINEX compliant template generator (feature extractor) or matcher, does the supplier still have to submit its product (software libraries) to GSA for approval?
Yes, in order to be included in the Approved Products List, suppliers must submit an application as required for the applicable Approval Procedure.

If a supplier is listed by NIST as having a MINEX compliant template generator (feature extractor) or matcher, will GSA perform any further evaluation of the actual software product libraries/SDK or will GSA limit its evaluation to a review of the application package, attestation and non-disclosure agreement for completeness and accuracy?
The GSA Evaluation Procedure for Template Generators and Template Matchers has been published at www.idmanagement.gov. Where documentation meets the requirements outlined in the procedure, no further evaluation is required.

Does GSA plan to evaluate mobile wireless readers for FIPS 201?
Mobile wireless readers contain a ‘reader’; therefore, these products should be submitted against the reader category for evaluation and inclusion on the approved products list.

If a product/service offering is on the SINs, does it need to be on the GSA approved lists?
All products on the SIN must also be on the GSA Approved Products List. Integration services are not listed on the approved products list; however, they must be qualified by GSA and must commit to delivering only products which have been approved and appear on the Approved Products List. For a listing of approved products and services, then refer to www.idmanagement.gov.

What is the GSA position on biometric sensor technology from an integration and interoperability perspective?
GSA categorizes biometric sensor technology by the FIPS 201 use cases. The interoperability issue is already addressed by NIST certifications of template management and template generators. Additional issues concerning the biometric middleware's ability to work with certain sensors are not addressed since biometric middleware is not a category at this time. Currently, middleware-to-sensor interoperability is the responsibility of the agency.

If biometric middleware is not an evaluation category, is not an agency in a situation in which they have to select components from a single vendor?
The mandate is to have data containers which are exchangeable throughout agencies. Biometric middleware is not considered to fall under this mandate. Agencies may choose to use different middleware-sensor pairing on different projects or at different sites.

Where can the list of product test plans and tested products, interoperability requirements, and the technical specifications be found?
For information on GSA Evaluation Program: http://www.idmanagement.gov.
For information on NIST conformance testing: http://csrc.nist.gov/npivp/.

Is it correct to qualify GSA testing as testing NIST-certified products interoperability between each other?
Not exactly. NIST validates 5 of the 24 FIPS 201 Product/Service categories that are critical to HSPD-12 security and interoperability objectives. GSA validates all categories as defined by FIPS 201 and supporting documentation. Interoperability is one of the goals of the evaluation program.

PRIVACY

Is a Privacy Impact Assessment (PIA) required for all agency data systems used to collect and store information related to the personal identity verification process?
Yes, a PIA is necessary.

How does FIPS 201 protect privacy?
During card issuance and life cycle management, all agencies are required to comply with FIPS 201, Section 2.4, "PIV Privacy Requirements," which outlines strict control measures to ensure the privacy of PIV card applicants and card holders is protected. In addition, Personally Identifiable Information (PII) stored on the card is minimal, as is PII acquired and retained by the issuance system. PII such as electronic fingerprints will be encoded as minutiae templates while stored on a PIV card. The PIV card, once activated, is in the control of the individual it identifies, who can then determine where and under what circumstances to present it.

FIPS 201 2.4 requires that all systems provide continuous auditing of privacy compliance covering collection, use, and distribution of information during program operation. Exactly what information needs to be recorded, how should it be recorded, and how should it be made available to the appropriate people?
Privacy Compliance is the responsibility of the Senior Agency Official for Privacy and should follow OMB guidance for privacy documentation.

Are there any specific requirements for when and/or how identity data should be protected, and who should or should not be able to access it? How does this requirement specifically affect communications with the IDMS and the FBI IAFIS for PIV-related fingerprint checks?
It is the responsibility of the Senior Agency Official for Privacy to ensure the identity data is properly protected from unauthorized disclosure. Agencies may use alternative methods for protecting information in transit and at rest. Interface specifications are under development and information on these may be accessed at http://www.idmanagment.gov. (Ref: FIPS 201, Section 2.4)

Do PIV systems require any specific support for limiting access to Information in Identifiable Form (IIF) beyond the standard login process? If so, what are the requirements?
No. Specific uses for the PIV security features are outside the scope of FIPS 201. Please refer to NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, and to FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, for recommendations on protection and access control for IIF.

SECURITY

How is security being improved by HSPD-12?
The standardization of identity proofing and vetting, and the implementation of a standardized identity credential that is tamper-resistant and can be rapidly verified electronically across Federal agencies will improve access control to Federal facilities and IT systems by providing a means to identify fraudulent or expired credentials and ensure the holder of the credential is the individual to whom it was issued. In addition, the PIV Card provides three factor authentication capability: something you have (the card with a PIV authentication certificate); something you know (the personal identification number or PIN); and something you are (the biometric).

What is a concise security policy statement that can be used for implementing and operating a PIV system?
One sample might be: “It is the policy of this organization to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by adopting and using procedures, components, and systems for secure and reliable identification and authentication of federal government employees and contractors (including contractor

employees and authorized affiliates) as specified in FIPS 201 and its supporting documents.”

TECHNICAL

What is the rationale behind the selection of smart card, fingerprint, and PKI technologies?
The presidential directive required a standard for secure and reliable identification and authentication of federal employees and contractors that incorporates rapid electronic validation, but did not specify how to achieve it. Several organizations (most notably DOD) had on-going smart card programs that demonstrated the efficacy of this technology in meeting the needs of HSPD-12. The decision to include PKI and fingerprint technologies was made to improve the security profile of the smart card for both physical and logical access. PKI provides a digital credential that can be used to electronically verify the identity of the cardholder, while the fingerprint ties the card irrevocably to a specific individual and can be used to ensure the cardholder is the individual to whom the card was issued. Of the several potential means of personal biometric marker verification (e.g., DNA, iris scans, hand geometry, handwritten signatures, facial images, or fingerprints), fingerprints were chosen as being the least invasive and most cost-effective, reliable, repeatable, and accurate means of verification available using publicly available technology.

What information must be stored on the card?
The PIV Card must contain the following mandatory Personally Identifiable Information:
1. Personal Identification Number (PIN)—this data is used to authenticate the cardholder to the card--in the same way a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card.
2. A Cardholder Unique Identifier (CHUID)—this number uniquely identifies the individual within the PIV system.
3. Two fingerprint biometrics that are PIN protected.
4. One asymmetric cryptographic key pair used to authenticate the card to the PIV system.

PIN Reset requires biometric authentication. Can this be accomplished remotely by providing unlock codes during in-person enrollment or issuance or is in-person appearance required?
For PIN resets, in-person appearance to authenticate identity is required. Identity authentication is accomplished through a biometric match to verify identity at the time of PIN reset. This is a security feature of the process. (Ref: FIPS201 Section 5.3.2.3)

If password manager products are considered a related subsystem, do these related subsystems need to be FIPS 201 compliant?
FIPS 201 does not specify password manager product requirements. However, where such products are considered PIV applications, the PIV authentication use cases in FIPS 201 Section 6 apply.

How should the PIV enrollment systems, issuance systems, and other clients communicate with and transfer these records to and from the Identity Management System (IDMS)?
A set of standard interfaces is currently being developed. Information on these can be found at http://www.idmanagement.gov.

Are PIV cards limited to the PIV card applications described by FIPS 201 or can additional applications and data objects be stored on the PIV card?
It is possible for a PIV card to contain non-PIV card applications, and those applications may contain non-PIV data objects. However, non-PIV applications and data objects cannot be used to supersede the operational use of the PIV application and data objects thereby hampering interoperability.

Should the PIV Data Model be considered fixed or can any Issuing Agency add more buffers (or containers) to meet their specific requirements?
New data objects may only be added to the PIV data model via formal revisions to the PIV standards and specifications, to ensure strict interoperability. In these cases NIST will assign new labels from the PIV namespace. However, it is possible to add proprietary data objects to non-PIV applications that reside on a PIV card.

TECHNICAL (BIOMETRIC)

Which fingers are required for capture on the PIV card. Should the choice of which fingers to capture for the PIV card be automatic, or should the operator have the final say?
The Index fingers are designated as primary for capture to the PIV card. Fingerprint substitution should only take place if the primary fingerprint cannot be imaged successfully (e.g. missing or badly scarred). (Ref: FIPS 201 Section 4.4.1)

In the event fingerprint capture is not possible, what should the alternative biometric be, and how should it be handled throughout the registration and issuance process?
In the event fingerprint capture is not possible, agencies must collect an alternative biometric. The most common is probably a facial image, however this is not specified by FIPS 201. For the purposes of the criminal history check, there is no alternate biometric. Where prints are not available, OPM will rely on the name check for criminal history. (Ref: FIPS 201 4.4.1)

What is the basis for the FIPS 201 fingerprint sensor requirement of 12.8mm x 16.5mm?
Computations made on data generated in NIST's MINEX trial showed that the best commercial template encoders access fingerprint ridge data in areas exceeding the final

12.8 x 16.5 specification. This finding implies some loss of minutia information if smaller areas are imaged.

At PIV card issuance, should the applicant's fingerprints be matched against the enrollment record, the PIV card biometrics, either, or both? Is this actually mandatory?
Biometric match of fingerprints at card issuance is mandatory. The match should be made against the templates placed on the PIV card from the record captured at enrollment. Whether this record is in the IDMS or on the PIV card is at the agency's discretion; however, matching to the PIV card has the added advantage of validating the biometric record on the PIV card. (Ref. FIPS 201, Section 5.3.1)

For fingerprint capture, is extraction from the record captured for the background investigation or independent capture the preferred method for collecting the PIV card fingerprint biometrics, and what are the restrictions on the use of either method?
Either method is acceptable. If capture is done independently, both capture events should be conducted in the same session to ensure continuity.

TECHNICAL (PKI)

Are there standards by which PKI Shared Service Providers must comply regarding RA/CA communication and key escrow?
PKI Shared Service Providers must comply with the Federal Common Policy Framework which details requirements for PKI operations. (http://www.cio.gov/ficc/documents/ CommonPolicy.pdf)

What is the relationship of a Device CA to the PIV trust model?
Device authentication is outside the scope of the Personal Identity Verification (PIV) program objectives. However, provisions have been made in the Federal Common Policy Framework for device certificates and agencies are encouraged to issue under this policy if interoperability with other Federal organizations is desired. (Ref: X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework)

FIPS-201, Section 5.4.2 states: "All certificates issued to support PIV Card authentication shall be issued under the Common Policy". Does this statement refer to all PIV-defined keys and their corresponding certificates?
Yes. The intent of this statement is that all certificates in the PIV data model shall be issued under the Common Policy.

Some of the specified ECC algorithms are patented by CertiCom and the Department of Defense has a licensing agreement for the use of patents in software development. What is the scope of this agreement for use implementing HSPD-12?
NSA has licensed the rights to 26 patents held by Certicom Inc. covering a variety of elliptic curve (EC) technology. Under the license, NSA has a right to sublicense vendors

building equipment or components in support of US national security interests. The NSA will not grant sublicenses to vendors who intend to sell their equipment for use in other areas such as the entertainment industry or general corporate security. These are not considered national security applications and are not eligible for the sublicense. To determine if the use of patented EC technology qualifies for a sublicense as a U.S. national security interest, contact the Business Affairs Office of the NSA/CSS Commercial Solutions Center. (Ref: http://www.nsa.gov/ia/industry/cep.cfm. Vendors may also contact Certicom directly to inquire about the NSA sublicense: http://www.certicom.com)

Both X.509v3 CRLs and OCSP are mandatory certificate status mechanisms. Under what circumstances would one status mechanism be preferred over the other or should both be used concurrently for all credential validation?
There is no scenario where a relying party is expected to check both the CRL and request status from an OCSP server. The relying party determines which status mechanism to use, based on the resources that are available in its environment. We might expect a physical access system for visitors to rely on OCSP responses, while an intra-agency application might function more efficiently using CRLs. Application developers may select the appropriate mechanism. Both CRLs and OCSP responses are digitally signed, and the FPKI will support ECC in addition to the RSA algorithms identified in 800-78. Relying parties that wish to maximize interoperability must verify signatures from both families. Systems with a limited community of users may choose to rely on a more limited set.

The FPKI Common Policy limits CA keys to a 6 year lifetime. Subscriber keys are limited to a maximum of half that (3 years). FIPS 201 allows credentials to be valid for up to 5 years. Given these facts, 5-year cards will require maintenance during their lifecycle (PIV certificate reissuance). Is this correct?
This is correct. To use a PIV card for the maximum five years, new PKI credentials will need to be obtained at the three year point. This is a security feature, as well as mitigating the risk of large CRLs. There are no plans to modify either FIPS 201 or the Common Policy. Technically, certificate renewal can be performed by the user from the desktop, or the agency may choose to re-issue smart cards every three years and align it with the PKI certificate issuance cycle.

Since legacy PKIs will initially be issuing PIV certificates that do not assert the id-CommonAuth policy object identifier (OID), do they need begin operating an On-line Certificate Status Protocol (OCSP) server as soon as they begin issuing PIV certificates, or can they wait until they begin issuing PIV certificates that include the CommonAuth policy OID?
A legacy PKI issuing PIV certificates needs to implement an OCSP server by January 1, 2008 or when the agency begins issuing certificates that assert id-CommonAuth policy OID, since these certificates must include the URL of the authoritative OCSP server.

Is more than one certificate permitted to be bound to the same public key?
No. Each public key in the PIV data model has only one certificate binding.